A Study on Key Management Protocol for Wireless Ad Hoc Networks

氏名（本籍地）	CHEN 陳 QING 青
学位の種類	博　士（情報科学）
学位記番号	情　博　第538号
学位授与年月日	平成24年3月27日
学位授与の要件	学位規則第4条第1項該当
研究科、専攻	東北大学大学院情報科学研究科（博士課程）応用情報科学専攻
学位論文題目	A Study on Key Management Protocol for Wireless Ad Hoc Networks （無線アドホックネットワークのための暗号鍵管理プロトコルに関する研究）
論文審査委員	（主査）東北大学教授　加藤　寧 東北大学教授　木下　哲男　　東北大学教授　曽根　秀昭

論文内容の要旨

Chapter 1. Introduction, Research Background and Objective

Mobile Ad hoc NETworks (MANETs) show an alternative way of communication, where wireless nodes cooperate with one another to forward packets from a source to the appropriate destination, in a multi-hop fashion. Each MANET node collects information from its one-hop neighbors. Thus, MANETs nodes do not need to know about the whole network topology. In other words, there is no need for a centralized infrastructure in a MANET. This design consideration for MANETs makes a number of differences to the conventional centralized networks, namely: a) dynamic topology; b) resource constraints; c) lower cost; d) limited physical security.

These features have their pros and cons in MANETs. For instance, MANET nodes are able to roam freely at certain speed. While this feature allows for sufficient flexibility in deploying a network, it may also lead to unpredictable situations whereby the nodes may move too far away and become isolated. On the other hand, MANET nodes may be notebook computers, cell phones or even PDAs that are usually suffer from relatively short battery life. In addition, MANETs are meant to be deployed swiftly without infrastructures (e.g., base stations or access points), which cuts considerable cost. Finally, MANETs suffer from limited physical security. This is due to the fact that mobile terminals (e.g., notebooks, PDAs, and so forth) usually do not have sufficiently strong secure hardware as they increase cost and power-consumption. Indeed, the usability and reliability of MANETs strongly depend on its security.

However, because of its openness and lack of centralized services, it is still quite an endeavor to create a secure environment for MANETs. The fact remains that it is quite difficult to ensure confidentiality and authenticity in MANETs.

MANET is subjected to a number of attacks, ranging from rather simple to sophisticated ones. For instance, a selfish node in the MANET may not be willing to route packets to others. It may also discard data packets that it received from other nodes. On the other hand, more sophisticated routing attacks against MANETs may

disrupt route discovery. Furthermore, they may disrupt the route maintenance by disobeying the routing protocols. Blackhole attack, Byzantine attack, wormhole attack, and spoofing attack are illustrations of various significant threats to MANETs.

For the purpose of secure group communications, cryptography has been incorporated into MANETs. Among the most popular techniques, Symmetric and Public Key Infrastructures are worth mentioning.

In the former, two or more users are able to establish secure communications by sharing a common secret key. However, in a MANET with a large number of nodes, private key agreement protocols tend to require numerous message exchanges, which consequently cause significant overheads. Public Key Infrastructure (PKI) employs a pair of keys to encrypt and/or decrypt the messages. While the private keys need to be kept secret by both parties, the public keys can be widely distributed. In addition, PKI reduces the communication overhead. However, deploying PKI in MANETs demands for a trusted third party as the Certificate Authority (CA). Providing an online CA presents an enormous technical challenge in a MANET due to its dynamic topology. As a consequence, the public key-based authentication service for the MANET should be both decentralized and autonomous.

To this end, we present a novel PKI-based key management protocol in this paper. The key management protocol ensures secure admission control in MANET environments. In our protocol, we assign the responsibilities of the authenticator to multiple CAs, which are selected from a pool of users with the highest trust levels. In our approach, we do not resort to manual selection of CAs as that in the work of MOCA. We rather employ a Certificate Graph (CG) to represent the friendship amongst the participants. Our approach is similar to human social networks in which good (i.e., non-malicious) users are expected to have more friends than bad (i.e., malicious) ones. The most trustworthy subset of these good users in a MANET is represented by the maximum clique and is selected as the authenticator of this group.

We introduce a novel key management protocol to perform admission control for MANETs. Inspiration comes from MOCA. We combine the benefits of both certificate graphs and CAs. By searching for the maximum clique in certificate graphs we find the most trustworthy nodes. Then we assign CA responsibilities to these clique nodes. The details of our proposed scheme are presented in the remainder of this section.

We justify the reasons for choosing the maximum clique as CA in a MANET as follows. First, maximum cliques are found by the MANET nodes themselves. Since they are not manually selected, this ensures a de-centralized and autonomous infrastructure suitable for MANET topologies. Second, in a mobile network with more than one CA, it is obvious that every CA should be familiar with the other CAs by knowing their public keys. Besides, certificates stored at different CAs must be consistent. Otherwise, the CAs may present conflicting certificates to one another. In a maximum clique derived from a given MANET topology, each member in the clique knows its other members. In other words, there doesn't exist two members that are stranger to each other. This ensures close cooperation amongst the CAs. In addition, the considered network may consist of both malicious and non-malicious users. For instance, some malicious users may be selfish and disrupt the packet routing. Similar to social networks, the good (i.e., non-malicious) users in a MANET are trusted by more nodes in the envisioned maximum clique based approach. On the other hand, the malicious users with lower trust levels are left with zero or few friendly neighbors to communicate with. Thus, by constructing the maximum clique, we actually establish the most trustworthy subset of the good users in the mobile ad hoc network.

To integrate admission control scheme into MANET, we extend AODV protocol with our key management function. In our proposed scheme, CA selection proceeds as the following three steps.

(1) Issuing certificate. The protocol begins with issuing of certificates. At this stage, users issue certificates for their trustworthy neighbors.

(2) Exchange of certificates. These certificates can be exchanged amongst the nodes, which are considered as friends. This is achieved by exchanging the certificate chain packets with friends.

(3) Searching for the maximum clique in CG. The result of issuing and exchanging certificates is a CG. With the CG, users can gain knowledge of their respective neighbors. By searching for the maximum clique in the CG, a user can find a subset of nodes, which are the maximum clique members. These maximum clique members are selected as CAs.

We use identity-based key exchange protocol from pairing for encryption. By using the CK model, we say that a key exchange protocol is secure if under the allowed adversarial actions it is impossible for the attacker to distinguish the value of a key generated by the protocol from an independent random value.

Chapter 2. Wireless Ad Hoc Network Architecture and Security Issues

In this chapter, we focus on the study of wireless ad hoc network. In such kind of network, wireless nodes cooperate with one another to forward packets from a source to the appropriate destination, in a multi-hop fashion. Each node collects information from its one-hop neighbors. Thus, wireless nodes do not need to know about the whole network topology. In other words, there is no need for a centralized infrastructure in such kind of network. This design consideration makes a number of differences to the conventional centralized networks. For instance, wireless nodes are able to roam freely at certain speed. While this feature allows for sufficient flexibility in deploying a network, it may also lead to unpredictable situations whereby the nodes may move too far away and become isolated. On the other hand, wireless nodes may be notebook computers, cell phones or even PDAs that are usually suffer from relatively short battery life. In addition, they are meant to be deployed swiftly without infrastructures (e.g., base stations or access points), which cuts considerable cost. Finally, they suffer from limited physical security. This is due to the fact that mobile terminals (e.g., notebooks, PDAs, and so forth) usually do not have sufficiently strong secure hardware as they increase cost and power-consumption. Indeed, the usability and reliability of the network strongly depend on its security.

Because of its openness and lack of centralized services, wireless ad hoc network is subjected to a number of attacks, ranging from rather simple to sophisticated ones. For instance, a selfish node in the network may not be willing to route packets to others. It may also discard data packets that it received from other nodes. On the other hand, more sophisticated routing attacks against the network may disrupt route discovery. Furthermore, they may disrupt the route maintenance by disobeying the routing protocols. Blackhole attack, Byzantine attack, wormhole attack, and spoofing attack are illustrations of various significant threats to the wireless ad hoc network.

Chapter 3. Public Key Infrastructure based Certification

In this chapter, we focus on the utilization of Public Key Infrastructure (PKI) for certification inside wireless ad hoc network. PKI employs a pair of keys to encrypt and/or decrypt the messages. While the private keys need to be kept secret by both parties, the public keys can be widely distributed. In addition, PKI reduces the communication overhead. However, deploying PKI in wireless ad hoc network demands for a trusted third

party as the Certificate Authority (CA). Providing an online CA presents an enormous technical challenge due to dynamic topology of the network. As a consequence, the public key-based authentication service for the wireless ad hoc network should be both decentralized and autonomous. To this end, we present a novel PKI-based key management protocol. We apply Certificate Graph (CG) and identity-based security in designing a security scheme for wireless ad hoc networks. We first use one-hop message exchange to build CG at each mobile node. Then we select maximum clique nodes in CG as distributed CAs.

Chapter 4. Message Authentication and Secure Session

In this chapter, we focus on the detail of message authentication of the proposed protocol. In data communication between any pair of nodes, we encrypt each session with a session secret key. We first describe the encrypted session. Then we prove the security using Canetti Krawczyk (CK) model. With the CK model, we say that a key exchange protocol is secure if under the allowed adversarial actions it is impossible for the attacker to distinguish the value of a key generated by the protocol from an independent random value.

In Chapter 5, we conclude the overall thesis and discuss the future works.

論文審査結果の要旨

無線端末が協力して目的ノードまでパケットを転送するマルチホップ通信を用いるモバイルアドホックネットワーク（MANET: Mobile Ad Hoc NETwork)は新たな通信方式として注目されている。MANET では、各端末が近隣ノードのみから情報を取得するため、ネットワーク全体を知る必要がない。言い換えれば、MANET は集中型の基盤を必要としないものである。

分散型の MANET は従来の集中型のネットワークとは次の点で異なる。（1）動的なトポロジ、（2）資源の制限、（3）安価なネットワーク構築、（4）物理的セキュリティによる脆弱性。開放性と分散性の２つの特徴を有する MANET のセキュリティは機密性と信頼性に依存するが、これらを保証する安全な環境構築は困難である。この問題に対して、本論文は、新しい認証の手法を提案し、解析およびシミュレーション実験により有用性を確認している。

本論文は全編５章からなる。

第１章は序論であり、本研究の背景と目的について述べている。

第２章では、攻撃に対する既存のアドホックネットワークプロトコルや普遍的なセキュリティ手法について詳しく述べている。さらに、攻撃に対応可能なアドホックネットワークプロトコルの重要性を指摘し、攻撃といった脅威に対応するための適切なアーキテクチャの必要性を述べ、本研究の基本的な考え方を示している。

第３章では、MANET における安全な通信を保証するいくつかの関連手法を示し、問題点を明らかにしている。続いて鍵の中央管理が困難なため、無線アドホックネットワークにおける認証基盤として、共通鍵暗号方式ではなく公開鍵暗号方式を導入している。さらに、認証グラフと認証局を結合したクリークに基づく分散型認証局を提案している。提案手法は認証グラフから最大クリークを探索することで最も信頼のおける端末を発見し認証局とするもので、既存の手法に比べて認証の性能が大きく向上していることをシミュレーションによって確認している。これは実用上大きな成果である。

第４章では、無線通信における安全な通信を保証するためのプロトコルを実装した暗号化アルゴリズムを詳細に述べている。また、いずれの端末間の通信においても、このアルゴリズムは通信を安全に暗号化できることを示している。具体的には Diffie-Hellman 鍵共有プロトコルとハッシュに基づくメッセージ認証符号をベースに Canetti Krawczyk モデルを用いて安全性を証明している。この成果はアドホックネットワークの安全通信に貢献するもので高く評価できる。

第５章は結論であり、本研究の成果をまとめている。

本論文では、MANET における安全な鍵管理方式を提案した。提案手法は分散型の認証でありながら高い認証率と短い反応時間を保証し、認証の失敗を減少させている。本研究の成果は応用情報科学並びに情報通信技術の発展に寄与するところが少なくない。

よって、本論文は博士（情報科学）の学位論文として合格と認める。